

Tilburg University

Function creep

Prins, J.E.J.

Published in:

Justitiële verkenningen: Documentatieblad van het Ministerie van Justitie

Publication date:

2011

Document Version

Publisher's PDF, also known as Version of record

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):

Prins, J. E. J. (2011). Function creep: Over het wegen van risico's en kansen. *Justitiële verkenningen: Documentatieblad van het Ministerie van Justitie*, 37(8), 9-21.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Function creep: over het wegen van risico's en kansen

*J.E.J. Prins**

Wie met alcohol in het verkeer de fout in gaat, loopt binnenkort het risico dat zijn auto wordt voorzien van een tweede slot, het zogeheten alcoholslot. Dit technische systeem moet voorkomen dat automobilisten die de wettelijk toegestane alcohollimiet ernstig of herhaaldelijk hebben overschreden, niet nogmaals in de fout gaan.¹ Bij een bepaald alcoholpromillage van de bestuurder start de auto namelijk simpelweg niet: de startblokkering kan alleen gedeactiveerd worden nadat de bestuurder in het slot heeft geblazen en blijkt dat hij niet meer dan de toegestane hoeveelheid alcohol heeft gedronken. Behalve de technische voorziening in de auto worden ter uitvoering van dit initiatief ook allerlei persoonsgegevens van de betrokken automobilisten geregistreerd en wel bij het Centraal Bureau Rijvaardigheidsbewijzen (CBR) en de Rijksdienst voor het Wegverkeer (RDW). Tijdens de behandeling van het wetsvoorstel inzake het alcoholslot was de CDA-fractie in de Eerste Kamer benieuwd naar de relatie tussen enerzijds deze registraties met gegevens over alcoholmisbruik in het verkeer en anderzijds het elektronisch patiëntendossier: 'Voorziet de regering op termijn een link naar het Elektronisch Patiënten Dossier (EPD) vanwege de mogelijke relatie tussen alcoholgebruik, medicijngebruik en rijvaardigheid?', was de vraag van de fractie.² De minister antwoordde: 'in een link tussen beide systemen wordt niet voorzien'.³ Alhoewel hij dat niet zo expliciet verwoordde, was zijn

* Prof. mr. Corien Prins is hoogleraar aan het Tilburg Institute for Law, Technology, and Society (TILT), Universiteit van Tilburg en Raadslid bij de Wetenschappelijke Raad voor het Regeringsbeleid (WRR). Deze bijdrage is voor een belangrijk deel ontleend aan het rapport iOverheid van de Wetenschappelijke Raad voor het Regeringsbeleid (maart 2011, zie: www.wrr.nl), dat onder haar verantwoordelijkheid werd opgesteld.

1 Kamerstukken II 2008/09, 31 896, nr. 1-3, Wijziging van de Wegenverkeerswet 1994 in verband met de aanpassing van de vorderingsprocedure en de invoering van het alcoholslotprogramma.

2 Kamerstukken I 2009/10, 31 896, B, nr. 4, Voorlopig verslag van overleg over Wijziging van de Wegenverkeerswet 1994.

3 Kamerstukken I 2009/10, 31 896, C, MvA – Wijziging van de Wegenverkeerswet 1994.

bijbehorende motivatie mede gestoeld op de uitgangspunten van ons privacyrecht. Maar waarom eigenlijk zouden we het EPD via een koppeling met de systemen van het CBR en de RDW niet ook een rol kunnen toedelen bij het tegengaan van alcoholmisbruik? Of andersom, het EPD niet verrijken met gegevens over alcoholmisbruik? Deze uitruil houdt toch de belofte in van zowel een verhoogde effectiviteit en efficiëntie bij het tegengaan van alcoholmisbruik als het verbeteren van de gezondheidszorg? En is de ultieme informatiesamenleving niet een transparante maatschappij, zoals Tsoukas (1997) ooit verwoordde? Bovendien, een overheid die innoveert, zou toch volop de kansen moeten kunnen benutten om 'informatiegestuurd beleid' te ontwikkelen, of dat nu op het terrein van de gezondheidszorg of de handhaving is? En dat verlangt dat we systemen ook kunnen verbinden met systemen die een geheel andere functie hebben. Kortom, innovatie is onlosmakelijk verbonden met *function creep*.

Twee zijden van een medaille

Van *function creep* spreken we niet alleen wanneer een systeem op een later tijdstip wordt verbonden met andere systemen die een andere functie hebben. Het is ook het proces waarbij een digitale applicatie of informatie die in eerste instantie functie X diende, gedurende de tijd ook voor functie Y of zelfs Z wordt aangewend. Het fenomeen lijkt een kind van deze tijd en welhaast onlosmakelijk verbonden met de samenleving waarin wij leven: een samenleving die ten volle vertrouwt op het gemak en de meerwaarde die digitalisering ons heeft te bieden.⁴ *Function creep* is enerzijds een sluipend proces, dat zich welhaast ongemerkt over een periode van jaren uitstrekt. Anderzijds heeft het ook een zekere voorspelbaarheid in zich. In politieke discussies wordt het vaak op gepaste afstand gehouden en formeel verworpen, in het volle besef dat de toekomst met een grote mate van waarschijnlijkheid precies datgene zal brengen wat op dat moment formeel wordt uitgesloten.

4 Natuurlijk bestaat het fenomeen van *function creep* al veel langer. Het is immers van alle tijden dat objecten, processen of procedures in een later stadium een heel andere toepassing krijgen dan waarvoor ze in eerste instantie ontworpen waren. Deze bijdrage beperkt de bespreking tot *function creep* bij het gebruik van digitale systemen en digitale informatie.

Een discussie over *function creep* brengt ons vaak bij het thema privacybescherming. Het noopt immers tot een debat over de ruimte die de Wet bescherming persoonsgegevens (Wbp) – en meer concreet het daarin neergelegde beginsel van doelbinding – biedt om een applicatie die in eerste instantie functie X dient, gedurende de tijd ook voor functie Y of zelfs Z aan te wenden. Of de mogelijkheid om systeem A op een later tijdstip te verbinden met systemen B en C, die een geheel andere functie hebben. In dit privacyperspectief figureert *function creep* veelal in problematische zin. Maar de medaille heeft ook een andere – meer optimistische – zijde: *function creep* als inherent kenmerk van innovatie. Een samenleving die optimaal en vooral efficiënt innoveert doet immers, hoe ze het ook wendt of keert, uiteindelijk aan *function creep*. Het netwerkarakter van informatietechnologie maakt het buitengewoon aantrekkelijk om aan allerhande systemen die in beginsel een bepaalde functie dienen ook een andere functie toe te voegen dan wel te verbinden met systemen die deze andere functie hebben. De mogelijkheden om via ICT gemakkelijk en snel al eerder verzamelde informatie opnieuw te gebruiken, houden de belofte in van een veilige samenleving waarin maatschappelijke risico's tijdig in beeld komen omdat informatie uit verschillende systemen effectief met elkaar in verband valt te brengen, en ook van een efficiëntere wereld die zich kenmerkt door optimaal (her)gebruik van systemen en verzamelde gegevens. *Function creep* kent kortom twee zijden van de medaille – kansen en risico's – waarbij beide zijden overigens soms vervelend dicht bij elkaar kunnen liggen.

De risicozijde van de medaille omvat veel meer dan alleen de vaak bediscussieerde privacyimplicaties. De vermenging van informatie, alsmede de bewerking en de decontextualisering daarvan – consequenties die inherent zijn aan *function creep* – hebben namelijk ook gevolgen voor (1) traditionele grenzen tussen beleidsterreinen en sectoren en (2) de kwaliteit en betrouwbaarheid voor informatie. Het zijn deze consequenties die in deze bijdrage centraal zullen staan. Vanuit deze insteek zal ik in de navolgende paragraaf allereerst enkele voorbeelden van *function creep* bespreken. Vervolgens richten we de blik op de consequenties van het fenomeen en zullen we vaststellen dat grenzen tussen beleidsterreinen (zorg, controle, dienstverlening) en sectoren (publieke en private sector) gaan schuiven en soms zelfs afbrokkelen. Ook constateren we dat *function creep* onherroepelijk van invloed is op de kwaliteit

en betrouwbaarheid van de informatie die in de nieuwe (opeenvolgende) functies wordt benut. De slotparagraaf rondt het betoog af met de constatering dat het noodzakelijk is beide zijden van de medaille voor ogen te houden. In de dagelijkse praktijk zal *function creep* zonder twijfel onverminderd doorgaan. De kanszijde van de medaille (innovatie) vraagt erom. Een absolute halt aan het fenomeen toeroepen is aldus niet aan de orde. We moeten echter evenmin de ogen sluiten voor de risicozijde van de medaille, wat kan betekenen dat *function creep* toch ook zo zijn grenzen kent.

Function creep in Nederland en Europa

Function creep is een proces dat zich vaak over jaren uitstrekt. Wie terug in de tijd gaat en initiële ambities rondom projecten afzet tegen huidige toepassingen, ontwaart vele voorbeelden. Een eerste voorbeeld is het burgerservicenummer (BSN), dat als 'sleutel' fungeert voor het uitwisselen van persoonsgerelateerde gegevens. Het gebruik van dit unieke centrale identiteitsnummer moet het uitwisselen van persoonsgerelateerde gegevens eenvoudiger en betrouwbaarder maken. Oorspronkelijk was het BSN bedoeld voor en dus beperkt tot de contacten die burgers met de overheid onderhouden.⁵ Inmiddels wenst een groeiend aantal partijen in de private sector ook gebruik te mogen maken van dit nummer en – in sommige gevallen – tevens van de aan dit nummer verbonden persoonsgegevens: 'VNO-NCW is verontrust over de tot nu toe gemiste kans om het wetsvoorstel inzake het Burgerservicenummer (BSN) ook van nut te laten zijn in de ondernemingsadministratie.'⁶ Het nummer mag al binnen de zorg worden gebruikt en er is een wetsvoorstel in voorbereiding voor het gebruik van het BSN in de financiële sector.⁷ In de zomer van 2010 ontstond een felle discussie tussen het College bescherming persoonsgegevens en het ministerie van Ver-

5 Voor een overzicht van de overheidsinstanties die het BSN met elkaar mogen uitwisselen, zie www.burgerservicenummer.nl.

6 VNO-NCW, Brief aan de leden van de Vaste Tweede Kamer Commissies voor Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken en Justitie, Den Haag, 28 oktober 2005, www.eerstekamer.nl/behandeling/20080303/brief_van_vno_ncw_aan_de_tweede/f=/w30312ibijl2.pdf.

7 Kamerstukken I 2009/10, 30 312, L, Brief staatssecretaris betreffende de toekenning, het beheer en het gebruik van het Burgerservicenummer.

keer en Waterstaat over het gebruik van het BSN op de Rijkspas (CBP, 2010). En bij het ministerie van Economische Zaken, Landbouw en Innovatie wordt onderzocht in hoeverre het nummer gebruikt kan worden in het kader van de elektronische herkenning (eHerkenning) van bedrijven en zelfstandigen zonder personeel bij digitale dienstverlening (Leenes e.a., 2010).

Het meest bekende en besproken voorbeeld in ons land van *function creep* is echter de toepassing van biometrie op het paspoort. Aanleiding vormde een Europese verordening die als doel had het paspoort beter te beveiligen tegen fraude. Ons land koos er bij de implementatie voor de applicatie ook in te zetten voor opsporingsdoeleinden en wel via de opslag van biometrische gegevens in een landelijke databank die hiervoor gebruikt kon worden (zie hierover Böhre, 2010). Waar de Tweede Kamer-fracties in eerste instantie over vrijwel de gehele breedte deze regeringsplannen steunden, toonden ze zich vanaf medio 2010 alsnog bezorgd:

'Er zijn reële risico's: fraude, function creep en verkeerd gebruik (...) Het is en blijft mij dan ook volstrekt onduidelijk waarom wij in Nederland zo nodig het voortouw hebben willen nemen en twee doelen in één wet hebben willen verenigen, namelijk het bestrijden van identiteitsfraude – een doel waar ik mij volledig in herken en wat ik ook wil – maar ook het opsporen van strafbare feiten, en dan met die database als verbindende factor.' (VVD-Kamerlid Hennis-Plasschaert)⁸

Migratiedatabanken

Ook op Europees niveau zijn voorbeelden van *function creep* te vinden, met het beleidsterrein van migratie als koploper (Lyon, 2007; Dijstelbloem en Meijer, 2009; Broeders, 2011). In de afgelopen twintig jaar is op Europees niveau een netwerk van databanken ontwikkeld en ingevoerd om migratie 'beheersbaar' te maken. De verleiding van *function creep* bleek daarbij groot: geen van de systemen is beperkt gehouden tot het doel waarvoor ze in eerste instanties waren opgezet. De geschiedenis van de migratiedatabanken laat bovenal zien dat bij de keuzes over de technologie bewust is voorgesorteerd op deze latere uitbreidingen

8 Kamerstukken II 2010/11, 25 764, nr. 44, p. 4, Algemeen Overleg over Nederlandse reisdocumenten.

en toevoegingen. Het Schengen Informatie Systeem (SIS) was van meet af aan zo populair dat al in 1996 werd besloten een SIS II-systeem te ontwikkelen. De ontwikkelingsfase loopt echter nog steeds en gaandeweg legden de lidstaten steeds weer nieuwe wensen op tafel, zoals het toevoegen van meer informatiecategorieën, vooral biometrie, en toegang tot de gegevens van nieuwe organisaties, in het bijzonder criminaliteits- en terrorismebestrijders. De Europese Commissie heeft zich uiterst pragmatisch opgesteld tegenover deze verlanglijstjes: in afwachting van de uitkomst van de politieke besluitvorming liet men een systeem ontwikkelen dat al aan deze wensen voldeed. Het systeem 'must be designed and prepared for biometric identification to be implemented easily at a later stage, once the legal basis allowing for the activation of such potential functionalities, has been defined'.⁹ Het in 2007 genomen politieke besluit over de functies van SIS II noemt vingerafdrukken en foto's, maar een onderzoeksrapport van het Britse House of Lords stelt dat het systeem ook geschikt zal zijn voor irisscans en DNA. Technisch kan het, nodig is 'slechts' de creatie van wettelijke ruimte.¹⁰ Een vergelijkbare uitbreiding van functies zien we bij Eurodac. Oorspronkelijk was dit opgezet om 'asielshoppen' tegen te gaan, maar het werd al snel aangevuld met doelstellingen om illegale migranten te identificeren. De functie om illegalen te 'checken' en identificeren was optioneel voor de lidstaten, maar al snel zo populair dat de Commissie in haar evaluatie van het systeem voorstelde om voortaan ook de data over illegale immigranten op te slaan, in plaats van alleen te controleren. De Europese initiatieven op het terrein van migratie vormen overigens gelijk een mooie illustratie dat *function creep* niet alleen binnen de toepassing van een specifiek systeem speelt, maar ook bij verbinden tussen systemen. Het Visa Informatie Systeem (VIS) wordt ontwikkeld met interoperabiliteit en synergie met de reeds bestaande of in ontwikkeling zijnde systemen als centraal aandachtspunt. VIS en SIS II vormen (nu nog) 'aparte containers', maar de database, de technische lay-out en zelfs de fysieke locatie voor de centrale database zijn hetzelfde. De technische inrichting is volledig

9 Europese Commissie, Ontwikkeling van het Schengeninformatiesysteem II en mogelijke synergie met een toekomstig visuminformatiesysteem (VIS), COM(2003)771 def., p. 16.

10 House of Lords, Schengen Information System II (SIS II), Report with evidence, 9th Report of Session 2006-7 of the House of Lords' European Union Committee, Londen, The Stationary Office Limited 2007.20, n. 43.

geschikt voor koppeling van de databases, waardoor verschillende informatiestromen met elkaar in contact zouden komen.

Grenzen worden diffuus

In de voornoemde voorbeelden was veelal sprake van een min of meer expliciete keuze voor *function creep*. Het optimisme over de ogenschijnlijk onbeperkte mogelijkheden van technologie en informatieverstrekking uit zich in veel contexten echter ook als sluimerende *function creep*. Beleidsmakers of verantwoordelijken binnen private ondernemingen benutten zonder al te veel discussie kort na de ontwikkeling van een systeem alweer nieuwe toepassingsmogelijkheden of omarmen nieuwe partners die zich met hun systemen ook kunnen aansluiten. De omvang en effecten van dergelijk hergebruik en koppelen lijken zich veelal te onttrekken aan het zicht van niet alleen het bredere publiek, maar ook van de verantwoordelijke actoren (overheid, organisaties en bedrijven) zelf. Ook lijkt er nauwelijks oog te zijn voor de meer fundamentele effecten wanneer gegevens verder worden gekoppeld, door verschillende domeinen stromen en opgaan in bredere informatienetwerken. Een eerste effect is dat grenzen tussen beleidsterreinen en sectoren diffuus worden. Informatie die is verzameld onder de noemer van dienstverlening, zorg dan wel veiligheid wordt in toenemende mate ook buiten die context gebruikt, gekoppeld en verwerkt. Illustratief voor het afbrokkelen van grenzen tussen beleidsterreinen is de Verwijsindex Risicjongeren (VIR). De VIR is niet alleen dienstbaar aan zorg, maar ook aan controle omdat de verwijsindex actoren uit beleidsterreinen van zowel zorg als controle bij elkaar brengt (Keymolen en Prins, 2010). Alhoewel de meerderheid van de betrokken professionals binnen de (jeugd)zorg werkzaam is, is de verwijsindex ook uitdrukkelijk een instrument voor professionals die primair een controlerende taak hebben, zoals de politie. Tekenend is ook het initiatief van de Veiligheidshuizen. Bij het overleg binnen het Veiligheidshuis kunnen instellingen aansluiten die zich daarvoor niet eerder zo centraal in het domein van zorg voor risicjongeren bevonden, zoals kinderopvang, speelpleinen, kredietbanken, Leger des Heils en naschoolse opvang, en daarmee zeggenschap verkrijgen buiten het domein waarin ze van oudsher opereren (Holvast en Bonthuis, 2010).

Hiernaast schuiven onder invloed van *function creep* ook de grenzen tussen publieke, semipublieke en private sector. Steeds vaker bijvoorbeeld winkelt de overheid voor de benodigde informatie in de gegevensverzamelingen in het private domein. In toenemende mate verlangt de overheid dat gegevens die in de private sector in eerste instantie voor commerciële dienstverlening zijn verzameld, aan de overheid worden verstrekt. Waarbij deze gegevens dan niet voor service, maar ten behoeve van *control* worden ingezet. Het afgelopen decennium zijn alleen maar meer wetten geïntroduceerd die deze mogelijkheden faciliteren, zoals de Wet vorderen gegevens, de Wet bewaren verkeers- en locatiegegevens en Europese regelingen voor de doorgifte van passagiersgegevens en bancaire (SWIFT) gegevens aan de Verenigde Staten. Maar naast publiek-private informatiestromen die door speciale wetten worden gelegitimeerd, blijkt er ook veel mogelijk door afstemming van onderaf. Als bijvoorbeeld een gemeentelijke Sociale Dienst fraude bij uitkeringen op het spoor wil komen, dan staat de Wbp naar de opvatting van het College bescherming persoonsgegevens in principe toe dat een bestandskoppeling met bijvoorbeeld het waterleidingbedrijf wordt gemaakt (CBP, 2006, p. 1). In al deze gevallen lopen door gestapeld gebruik van informatie service (in dit geval van de private sector) en *control* (publieke sector) in elkaar over.

Zorgpunt: kwaliteit van informatie

Function creep is ook van invloed op de gegevens die onderwerp van hergebruik zijn en wel op het karakter, de betrouwbaarheid, de kenbaarheid, de contextualiteit en herleidbaarheid van informatie. De geschetste tendens van onbezorgd koppelen van informatiebestanden en overschrijden van domeinafbakeningen (dienstverlening, zorg en controle) – kortom hergebruik op hergebruik – kan niet anders dan het risico met zich meebrengen dat de kwaliteit van de informatie verwatert. Kenmerkend voor *function creep* is dat informatie wordt gedecontextualiseerd (uit de oorspronkelijke informatieomgeving gehaald) om vervolgens te worden gehercontextualiseerd (te worden gecombineerd met andere gegevens in een andere beleidscontext). Dat verlies van oorspronkelijke context heeft in potentie gevolgen voor de betrouwbaarheid en de kenbaarheid van informatie. Bovendien, naarmate de kwaliteit van

informatiebestanden verwatert, zorgen netwerken ervoor dat de risico's die samenhangen met het kwaliteitsverlies exponentieel groeien. Het gebrek aan kwaliteit van informatie onttrekt zich, juist in vernetwerkte situaties, maar al te gemakkelijk aan het zicht, zonder dat hiervoor altijd direct een 'schuldige' is aan te wijzen. Eerder is dit een onvermijdelijk risico van wat als het multipliereffect van ICT kan worden aangeduid: niet alleen correcte informatie heeft een enorme omloopsnelheid en effectieve distributie gekregen, maar ook foutieve informatie. De administratieve werkelijkheid en de 'werkelijke werkelijkheid' kunnen dan veel sterker uiteenlopen dan voorheen, en fouten kunnen zich bovendien veel sneller verspreiden, waarna ze – zo tonen ons de voorbeelden van identiteitsfraude – vervolgens veel moeilijker te herstellen zijn. Die fouten hebben in het dagelijkse leven soms grote gevolgen voor individuele burgers (zie hierover Buruma, 2011).

Ten slotte: het WRR-rapport iOverheid

Het enthousiasme voor *function creep*, kortom voor nieuwe toepassingen van bestaande applicaties en daarmee verband houdende koppelingen van systemen en informatiestromen, gaat hand in hand met argumenten als het vergroten van de veiligheid en het verhogen van effectiviteit en efficiëntie. Her- en verder gebruik wordt enthousiast omarmd voor zowel de complexe administratieve opdracht van organisaties als de aanpak van urgente maatschappelijke uitdagingen, zoals terrorisme, veiligheid, mobiliteit en goede en betaalbare zorg, of het behalen van economische voordelen, zoals nieuwe onlinedienstverlening op maat. En per beslissing om in een individuele situatie *function creep* de ruimte te geven blijken deze belangen in de regel zwaarder te wegen dan waarden als privacy, maar ook dan belangen als kwaliteit van informatie of de consequenties van de vermenging tussen service, *care* en *control* en de toenemend diffuse grenzen tussen publiek-private informatiestromen.

De geschetste consequenties en risico's rondom *function creep* sluiten nauw aan bij de analyse van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in het in het voorjaar 2011 gepresenteerde rapport *iOverheid*. Gegeven deze analyse bepleit de raad een grotere verantwoordelijkheid voor de overheid op ICT-gebied. De huidige

ontwikkelingen leveren simpelweg te veel risico's en knelpunten op. Niet alleen de overheid, maar ook bedrijven en organisaties raken (mede onder invloed van *function creep*) op het niveau van informatiestromen verknoopt, terwijl ze dat op organisatorisch en institutioneel niveau zeker niet zijn. De op digitaal niveau verknoopte samenleving kent daarmee een informatierealiteit die slecht aansluit bij de manier waarop organisaties, bedrijven, ministeries, toezichthouders, rechtsbeschermings- en klachtenprocedures zijn ingericht. Met als gevolg dat burgers niet weten waar in die gekoppelde wereld verantwoordelijkheid is belegd. En met als gevolg een serieus risico dat actoren binnen zowel de publieke als de private sector het regisserend vermogen kwijtraken.

De WRR bepleit daarom een inhoudelijk andere oriëntatie. De aandacht moet worden verlegd naar de vernetwerkte informatie-huishouding van onze samenleving. Voor het specifieke onderwerp van deze bijdrage luidt de boodschap vanuit deze andere oriëntatie dan: als we enerzijds accepteren dat *function creep* als zodanig een gegeven is vanuit de constatering dat het onlosmakelijk is verbonden met de noodzaak tot innovatie, maar anderzijds vaststellen dat het ook duidelijke risico's in zich draagt (behalve de in deze bijdrage genoemde risico's is dat ook privacy), zal nagedacht moeten worden over de grenzen aan *function creep*. Dat impliceert dat de zekere voorspelbaarheid van *function creep*, veel meer dan nu het geval is, expliciet gemaakt moet worden. Ook zullen burgers, zo stelt de WRR, veel meer dan nu het geval is in staat moeten worden gesteld een *countervailing power* te zijn. Daartoe is meer openheid van zaken bij de digitale overheid nodig. Zonder transparantie, en zeker ook inzicht, is reëel inzicht in en toezicht op *function creep* immers vrijwel onmogelijk. De burger in de rol van toezichthouder veronderstelt waakzaamheid en assertiviteit bij burgers die daartoe echter ook meer transparantie aan de kant van de overheid zouden mogen verwachten.

Inmiddels heeft het kabinet eind oktober 2011 in reactie op het WRR-rapport laten weten inderdaad werk te willen maken van meer transparantie.¹¹ Onderzocht zal worden, zo stelt het kabinet, of de webpagina MijnOverheid uitgebreid kan worden met

11 Kamerstukken II 2011/12, 26 643, nr. 211, p. 11-12, Kabinetsreactie WRR-rapport Overheid.

'inzage in de gegevens die de overheid over de burger heeft; inzage in het gegevensverkeer tussen overheidsorganisaties (welke gegevens over mij worden tussen welke organisaties uitgewisseld); een mogelijkheid tot verzoeken om correctie van onjuiste gegevens; een mogelijkheid om eigen gegevens op eigen verzoek actief te delen met derde partijen'.

Als transparantie inderdaad in deze mate gestalte krijgt, zal ook *function creep* uiteindelijk inzichtelijker worden. Immers, 'inzage in het gegevensverkeer tussen overheidsorganisaties (welke gegevens over mij worden tussen welke organisaties uitgewisseld)' zal burgers daartoe zeker de nodige aanknopingspunten opleveren. Toch is transparantie slechts één kant van de medaille. Met alleen transparantie worden de burger immers wel de nodige aanknopingspunten geboden voor meer inzicht in de informatieprocessen van de overheid, maar is allesbehalve gegarandeerd dat er werkelijk een zorgvuldig debat over maatvoering bij *function creep* wordt gevoerd. Dat debat verlangt in ieder geval dat er meer aandacht komt voor het evalueren van *function creep* en met name de parameters aan de hand waarvan de (geclaimde) 'kosten en baten' daarvan inzichtelijk kunnen worden gemaakt. Dat debat verlangt ook dat de motieven voor *function creep* daadwerkelijk geëxpliciteerd worden, waarmee ook duidelijker wordt wat de principiële tegenstellingen zijn die bij initiatieven tot *function creep* spelen. En hoe daarover wordt besloten. Want *function creep* is nooit alleen maar 'halleluja'. En ook nooit alleen maar negatief.

Literatuur

Böhre, V.

Happy landings? Het biometrische paspoort als zwarte doos

WRR-Webpublicatie nr. 46,
Den Haag, 2010, (www.wrr.nl)

Broeders, D.

Grensoverschrijdende mobiliteit van personen en de digitale grenzen van Europa

In: D. Broeders, C.M.K.C. Cuijpers en J.E.J. Prins (red.), *De staat van informatie*, WRR-verkenning nr. 25, Amsterdam, Amsterdam University Press, 2011, p. 245-288 (www.wrr.nl)

Buruma, Y.

Het recht op vergetelheid. Politieke en justitiële gegevens in een digitale wereld

In: D. Broeders, C.M.K.C. Cuijpers en J.E.J. Prins (red.), *De staat van informatie*, WRR-verkenning nr. 25, Amsterdam, Amsterdam University Press, 2011, p. 165-218 (www.wrr.nl)

College bescherming persoonsgegevens (CBP)

Notitie fraudebestrijding door bestandskoppeling

Den Haag, september 2006

College bescherming

persoonsgegevens (CBP)

Onderzoek naar de verwerking van het burgerservicenummer en kopie identiteitsbewijs voor de Rijkspas door de minister van Verkeer en Waterstaat

27 mei 2010 (www.cbpweb.nl/Pages/med_20100607_rijkspas.aspx)

Dijstelbloem, H., A. Meijer

De migratiemachine. De rol van technologie in het migratiebeleid

Amsterdam, Van Gennep, 2009

Holvast, J., M.J. Bonthuis

Blackbox-onderzoek

Veiligheidshuizen

WRR-Webpublicatie nr. 49, 2010, p. 32-33 (www.wrr.nl)

Keymolen, E.L.O., J.E.J. Prins

Jeugdzorg via systemen. De verwijzindex risicjongeren als spin in een digitaal vangnet

In: D. Broeders, C.M.K.C. Cuijpers en J.E.J. Prins (red.), *De staat van informatie*, WRR-verkenning nr. 25, Amsterdam, Amsterdam University Press, 2011, p. 289-344

Leenes, R.E., B.J. Koops e.a.

Onderzoek naar het gebruik van het Burgerservicenummer (BSN) binnen de keten van de elektronische dienstverlening tussen de overheid en bedrijven.

Tilburg, TILT, 2010

Lyon, D.

Surveillance studies. An overview
Cambridge, Polity Press, 2007

Tsoukas, H.

The tyranny of light. The temptations and the paradoxes of the information society
Futures, jrg. 29, nr. 9, 1997,
p. 827-843

**Wetenschappelijke Raad voor
het Regeringsbeleid (WRR)**

iOverheid

WRR-rapport nr. 86, Den Haag,
2011 (www.wrr.nl)